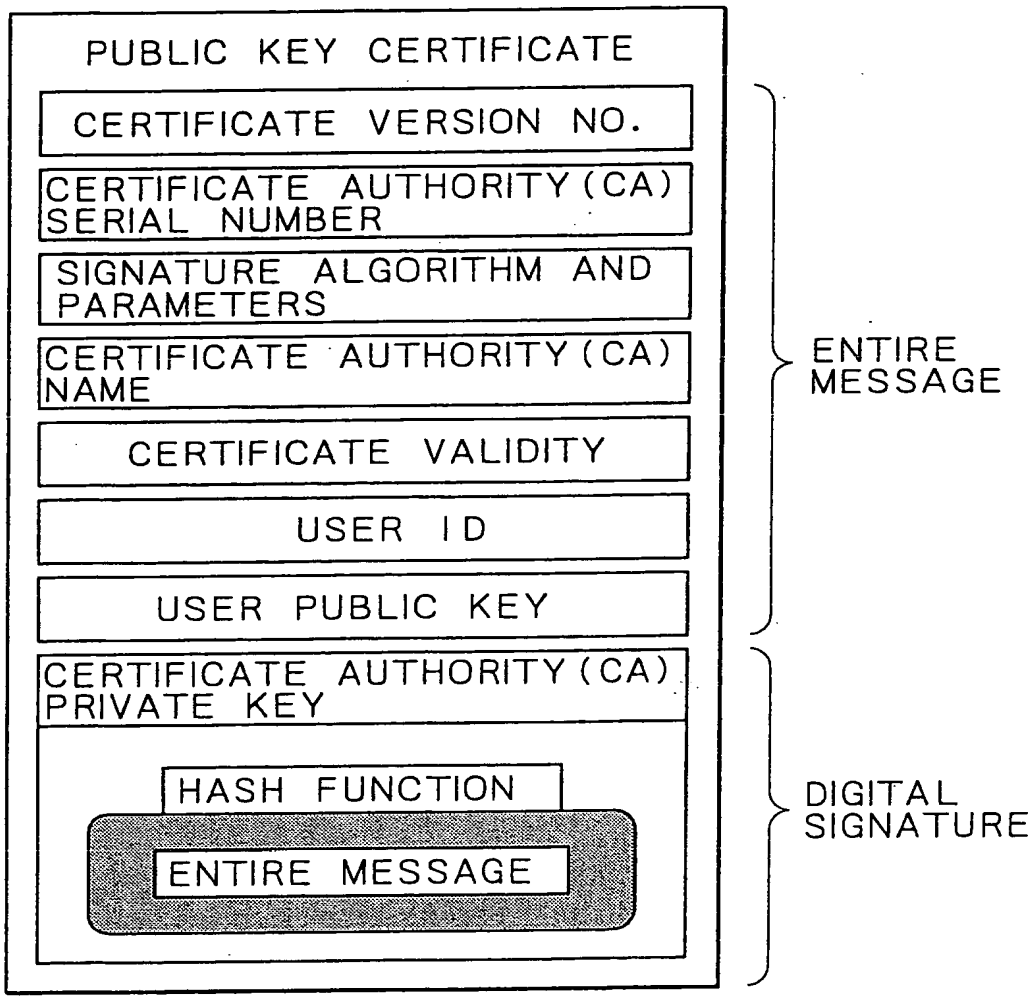
FIG. 1



PRIOR ART

FIG. 21A

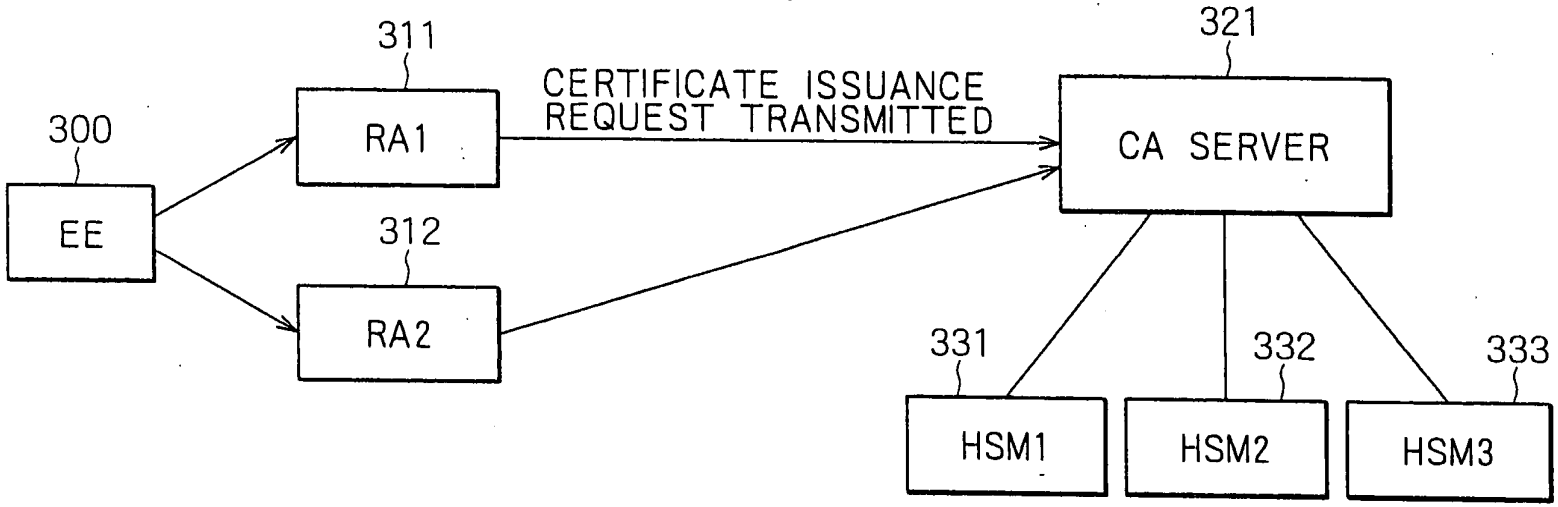


FIG. 21B

RA MANAGEMENT DATABASE

RA ID	USAGE OF MULTIPLE-SIGNATURE ALGORITHM	SIGNATURE ALGORITHM	KEY LENGTH	PARAMETERS	LOAD DISTRIBUTION	HSM IN USE
RA1	×	RSA	1024 bits	—	×	HSM1
RA2	○	RSA	2048 bits	—	×	HSM2
RA2	○	ECDSA	192 bits	p=XX,...	×	HSM3
RA2	○	ECDSA	192 bits	p=YY,...	×	HSM3

FIG. 21C

VERIFICATION KEY DATABASE

HSM ID	SIGNATURE ALGORITHM	KEY LENGTH	PARAMETERS	VERIFICATION KEY
HSM1	RSA	1024 bits	—	◇
HSM2	RSA	2048 bits	—	◆
HSM3	ECDSA	192 bits	p=XX,...	△
HSM3	ECDSA	192 bits	p=YY,...	▲

REPLACEMENT SHEET

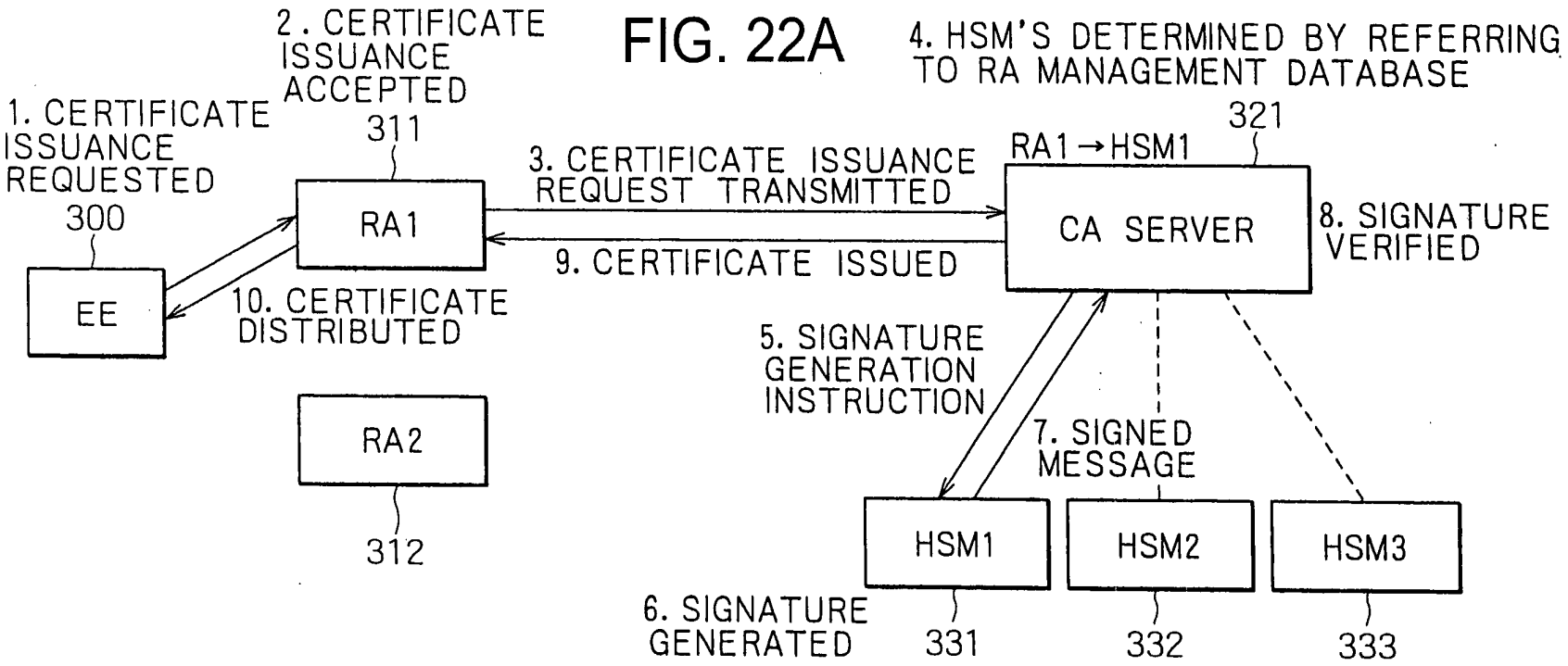


FIG. 22A

CERTIFICATE ISSUANCE REQUEST

COMMAND	MESSAGE	RA ID
CERTIFICATE ISSUANCE	Message1	RA2

FIG. 22B

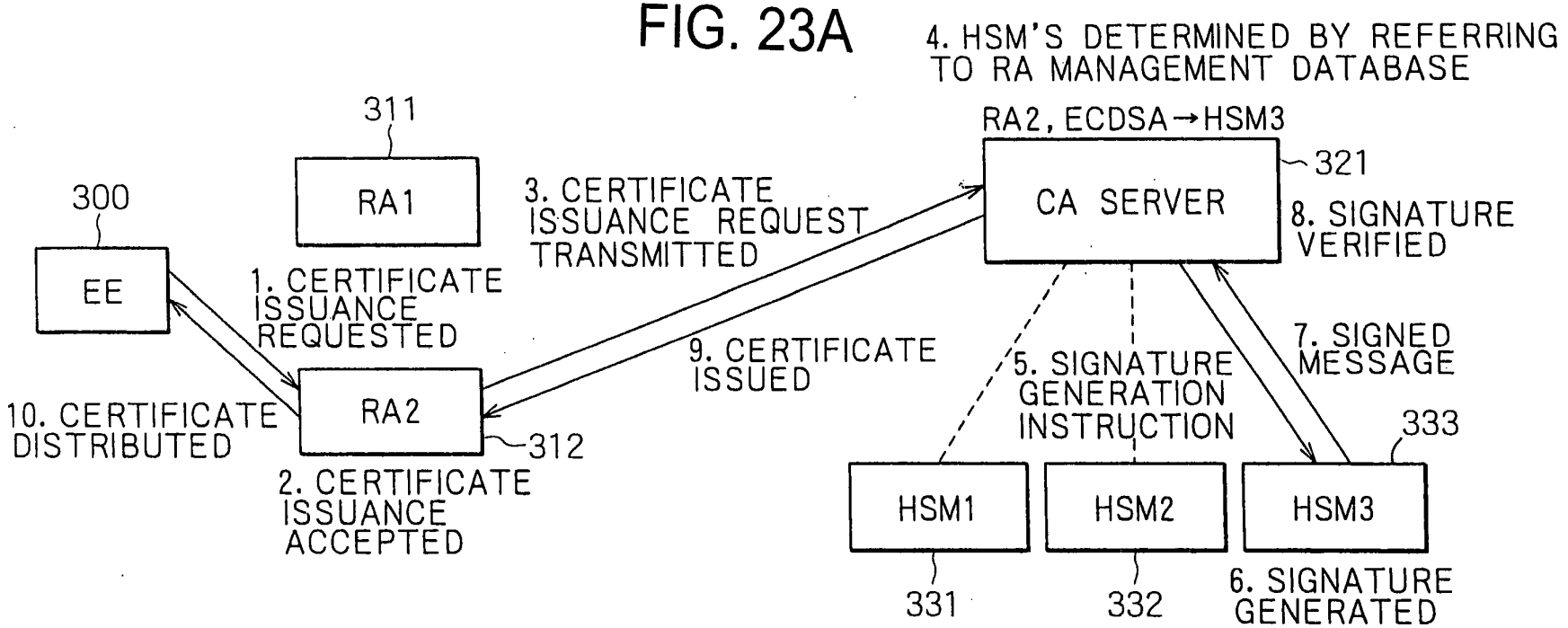
SIGNATURE GENERATION INSTRUCTION

COMMAND	MESSAGE
SIGNATURE GENERATION	Message1

FIG. 22C

REPLACEMENT SHEET

FIG. 23A



CERTIFICATE ISSUANCE REQUEST

COMMAND	MESSAGE	RA ID	SIGNAL ALGORITHM	KEY LENGTH	PARAMETERS
CERTIFICATE ISSUANCE	Message2	RA2	ECDSA	192 bits	p=XX,...

FIG. 23B

SIGNATURE GENERATION INSTRUCTION

COMMAND	MESSAGE	KEY LENGTH	PARAMETERS
SIGNATURE GENERATION	Message2	192 bits	p=XX,...

FIG. 23C

REPLACEMENT SHEET

FIG. 24 A

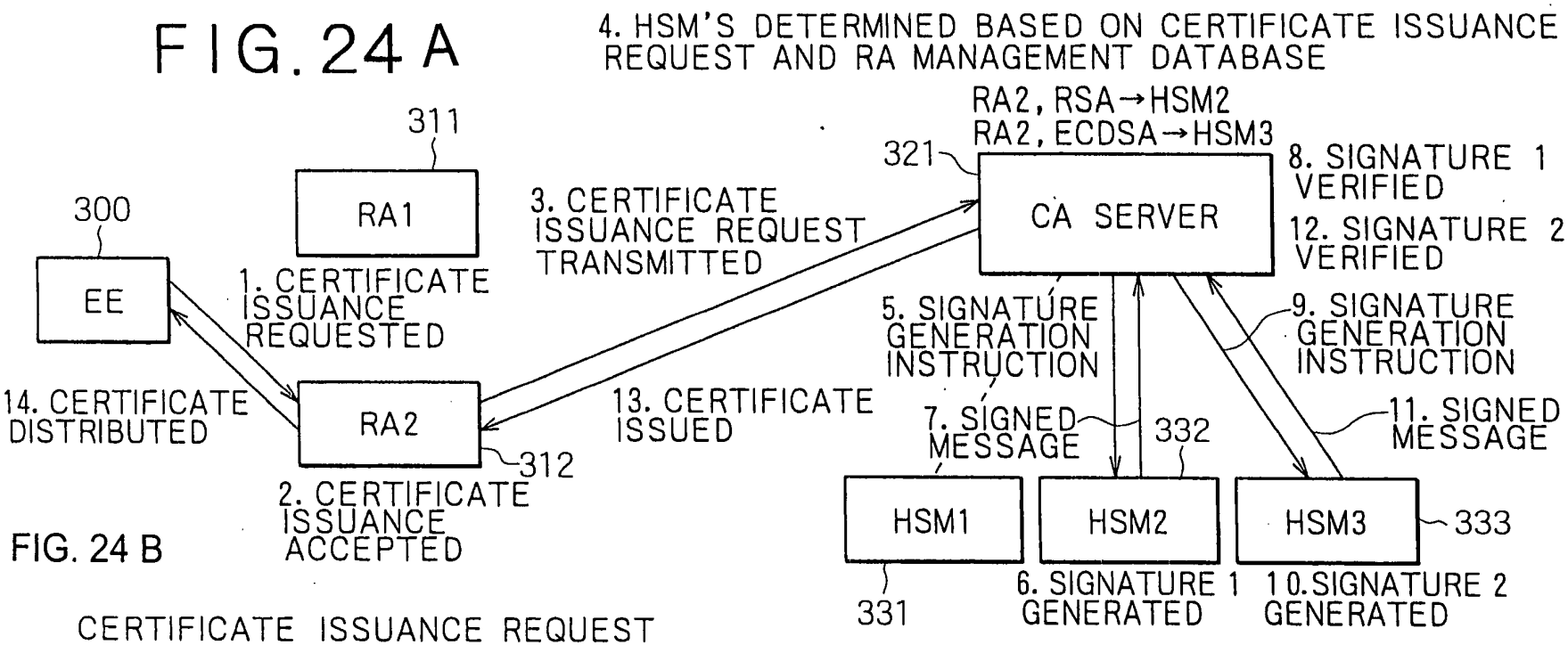


FIG. 24 B

CERTIFICATE ISSUANCE REQUEST

COMMAND	MESSAGE	RA ID	SIGNATURE ALGORITHM 1	KEY LENGTH	SIGNATURE ALGORITHM 2	KEY LENGTH	PARAMETERS
CERTIFICATE ISSUANCE	Message3	RA2	RSA	2048 bits	ECDSA	192 bits	p=XX,...

SIGNATURE GENERATION INSTRUCTION

COMMAND	MESSAGE	KEY LENGTH
SIGNATURE GENERATION	Message3	2048 bits

FIG. 24 C

SIGNATURE GENERATION INSTRUCTION

COMMAND	MESSAGE	KEY LENGTH	PARAMETERS
SIGNATURE GENERATION	Message3	192 bits	p=YY,...

FIG. 24 D

REPLACEMENT SHEET